

04/07/00
JC712 U.S. PTO

04-10-02
A

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Inventors: SPIELMANN, Craig
HUTTER, Maria
KLEIN, Joel
SINGHANI, Naresh

Filed: Herewith

Title: Method And System For Managing Risks

Attorney Docket No. JPM-001

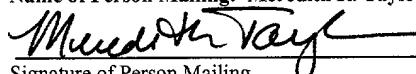
CERTIFICATE OF MAILING UNDER 37 CFR § 1.10
"Express Mail" Mailing Label Number

EL 577174616US

Date of Deposit: April 7, 2000

I hereby certify that this paper and all enclosures referred to therein are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR § 1.10 on the date indicated above with sufficient postage in an envelope addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231

Name of Person Mailing: Meredith R. Taylor



Signature of Person Mailing

JC511U545381 PTO
04/07/00


PATENT APPLICATION TRANSMITTAL LETTER

Assistant Commissioner for Patents
BOX PATENT APPLICATION
Washington, D.C. 20231

Sir:

Transmitted herewith are the following:

Specification, including claims, abstract and ten figures (37 pages),

Combined Declaration and Power of Attorney

Return receipt postcard.

Fees

Basic Fee			
Total Claims	18		
Indep. Claims	4		
Multiple Dependent Claim(s):			

SMALL ENTITY	
Rate	Fee
	\$
x 9.00	\$
x 39.00	\$
	\$ 0
TOTAL:	\$

OTHER	
Rate	Fee
	\$ 690.00
x 18.00	\$
x 78.00	\$ 78.00
	\$
TOTAL	\$ 729.00

The Commissioner is hereby authorized to charge the filing fee and any fees which may be required in connection with this submission, to **Deposit Account No. 19-2385**. (Please reference attorney docket no. JPM-001).

Date: April 7, 2000

Respectfully submitted,

By: 
 Andrew Strobert
 Registration No. 35,375
 SKADDEN, ARPS, SLATE, MEAGHER
 & FLOM LLP
 Four Times Square
 New York, New York 10022
 (212) 735-3000

METHOD AND SYSTEM FOR MANAGING RISKS

Field of the Invention

The present invention relates to a method and system for managing risks inherent in business activities and more particularly to a data processing apparatus and method for identifying, managing and quantifying risks and associated control procedures.

Background of the Invention

Many organizations worldwide have developed practices for internal control. The Institute of Internal Auditors' ("IIA") Standards for the Professional Practice of Internal Auditing (Standards) defines control as:

...any action taken by management to enhance the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient actions to provide reasonable assurance that objectives and goals will be achieved.
(Section 300.06)

According to Specific Standard 300.05, the primary objectives of internal control are to ensure:

1. The reliability and integrity of information.
2. Compliance with policies, plans, procedures, laws, regulations, and contracts.
3. The safeguarding of assets.

4. The economical and efficient use of resources.
5. The accomplishment of established objectives and goals for operations or programs.

5

Many organizations have recognized the need for tracking the effectiveness of internal control practices. For example, according to the IIA's Professional Practices Pamphlet 97-2, Assessing and Reporting on Internal Control, the IIA supports the Committee of Sponsoring Organizations of the Treadway Commission, recommendation that organizations should report on the effectiveness and efficiency of the system of internal control.

One system of internal control, the Control Self-Assessment (CSA) methodology, was initially developed in approximately 1987 and is used by many organizations to review key business objectives, risks involved in achieving objectives, and internal controls designed to manage those risks. The IIA states that some CSA proponents have expanded this description to encompass potential opportunities as well as risks, strengths as well as weaknesses, and the overall effectiveness of the system in ensuring that the organization's objectives are met.

20

CSA approaches and formats may differ from one organization to another, however, the three primary CSA approaches are: facilitated team meetings (also known as workshops), questionnaires and management-produced analysis. Organi-

zations may combine more than one approach. Facilitated team meetings gather internal control information from work teams that may represent multiple levels within an organization. The questionnaire approach uses a survey instrument that offers opportunities for simple yes/no or have/have not responses. Management-produced analysis is any approach that does not use a facilitated meeting or survey.

5 While existing methodologies and systems, such as the CSA, offer some structure in approaching the control of risk, to date, no system or methodology known to the applicants exists that properly quantifies risks and the effectiveness of 10 control procedures designed to address such risks. For example, many existing systems rely on a single weak link approach, without consideration of the significance 15 of such link. If an assessor utilizing the weak link approach identifies a large number of processes associated with a risk element (e.g. business continuity), the presence of a single non-complaint process would red-flag the entire risk element, regardless of the significance of the non-complaint process. Thus, existing systems provide no mechanism for comparing results over time, nor are they reliable for 15 providing a meaningful index of how well individual entities are measuring risk.

The method and system of the present invention addresses these and other limitations by utilizing a quantitative weighted approach to evaluating risk. A three-

tiered approach to evaluate risk is preferably used, dividing the system into: "Risks", "Subrisks," and "Control Procedures." An assessor is prompted through a series of screens to rate risks as "High," "Medium" and "Low." At the next level (the "Subrisk" level), a set of control procedures is provided. Each control procedure is rated by the assessor according to a number of categories, such as GREEN (full compliance), YELLOW (partial compliance), RED (non-compliance), or BLUE (not applicable). Control Procedures are assigned different weights because some risks are more critical than others. For items which are not fully compliant (e.g. items rated either YELLOW (partial compliance) or RED (non-compliance)), the assessor must either indicate that the risk is acceptable or create an action plan where deliverables are identified and target dates are established.

The system further provides a method of weighing, sorting and graphing displays which allows management to more easily identify significant areas of risk. This allows assessors to sort and view data in a number of ways, such as toy organization, business line, city and process. The display system further allows the user to "drill down" by clicking on high risk areas facilitating the identification of specific assessments which are having a significant impact on the risk rating.

Targets are derived from the Action Plans. A target is an index or measure which informs management of progress against action plans. Targets and actual

results will be compared from quarter to quarter, to determine whether appropriate progress is being made against commitments.

Brief Description of the Figures

These and other aspects of the present invention are more apparent in the following detailed description and claims, particularly when considered in conjunction with the accompanying drawings showing a system constructed in accordance with the present invention, in which:

Figure 1 is a system diagram showing the components of an exemplary system implementing the present invention;

Figures 2 is a logic diagram showing a preferred embodiment of the risk management system of the present invention;

Figure 3 is an exemplary computer display for rating the importance of a set of risk elements;

Figure 4 is an exemplary computer display showing subrisks, control procedures, compliance ratings and an action plan for non-fully complaint risks;

Figure 5 is an exemplary computer display for accepting risks or entering action plans;

Figure 6 is an exemplary computer display showing overall compliance scores sorted by business process;

Figure 7 is an exemplary computer display showing compliance scores for a specific subrisk sorted by city;

Figure 8 is an exemplary computer display showing a forecast report sorted by city and subrisk;

5 Figure 9 is an exemplary computer display showing actual versus target compliance scores sorted by subrisk; and

Figure 10 is an exemplary computer display showing an action plan count sorted by process and city.

Detailed Description of the Invention

10 Figure 1 depicts the components of an exemplary computing system implementing the inventive system for managing risk. Server 101 includes one or more communications ports 109 for communicating with assessors utilizing client workstations 108. Server 101 is coupled to one or more storage devices 103. Storage device(s) 103 include an executable or interpretable program 104 for controlling the management system. Storage device(s) 103 also include a rating database 105 containing data elements necessary for the rating process, and a quarterly assessment database 106 containing data elements necessary for quarterly assessments.

Figure 2 presents an overview of the inventive process of categorizing, weighing and tracking risks. Initially, a set of risk elements are identified 201. The following are exemplary risks in the field of investment management: (i) Business continuity, (ii) Financial, (iii) Information, (iv) Legal/Regulatory, (v) People, (vi) Physical Security, and (vii) Technology, however the set of risk elements will vary from application to application. Each risk is rated 202 preferably according to a fixed set of criteria. In the preferred embodiment of the invention these criteria comprise the probability of occurrence and the impact to the business should the situation occur. Each risk is also preferably rated by a fixed set of rankings, such as "High," "Medium" and "Low." Figure 3 is an exemplary computer display showing the rating 301 of risk elements 302 as High, Medium or Low. Each of these ratings 301 is stored in rating database 105 with the associated risk elements 302. Although not used in the preferred embodiment of this invention, these criteria and rankings may optionally be used in the weighing formula discussed below.

15 Each subrisk of the risk elements is identified 203 and presented to the user.

In the preferred embodiment, these subisks comprise:

1. Business Resumption:
 - i. Business Resumption; and
 - ii. Viruses.
2. Financial:
 - i. Expense Management.

3. Information:

- i. Restoration; and
- ii. Security.

4. Legal/Regulatory:

- i. Vendor Management; and
- ii. Software Licensing.

5. People:

- i. Capabilities; and
- ii. Compliance.

10 6. Physical Security:

- i. Physical access.

7. Technology:

- i. Change management;
- ii. Problem management;
- iii. Strategy; and
- iv. Dependability

15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
100
105
110
115
120
125
130
135
140
145
150
155
160
165
170
175
180
185
190
195
200
205
210
215
220
225
230
235
240
245
250
255
260
265
270
275
280
285
290
295
300
305
310
315
320
325
330
335
340
345
350
355
360
365
370
375
380
385
390
395
400
405
410
415
420
425
430
435
440
445
450
455
460
465
470
475
480
485
490
495
500
505
510
515
520
525
530
535
540
545
550
555
560
565
570
575
580
585
590
595
600
605
610
615
620
625
630
635
640
645
650
655
660
665
670
675
680
685
690
695
700
705
710
715
720
725
730
735
740
745
750
755
760
765
770
775
780
785
790
795
800
805
810
815
820
825
830
835
840
845
850
855
860
865
870
875
880
885
890
895
900
905
910
915
920
925
930
935
940
945
950
955
960
965
970
975
980
985
990
995
1000
1005
1010
1015
1020
1025
1030
1035
1040
1045
1050
1055
1060
1065
1070
1075
1080
1085
1090
1095
1100
1105
1110
1115
1120
1125
1130
1135
1140
1145
1150
1155
1160
1165
1170
1175
1180
1185
1190
1195
1200
1205
1210
1215
1220
1225
1230
1235
1240
1245
1250
1255
1260
1265
1270
1275
1280
1285
1290
1295
1300
1305
1310
1315
1320
1325
1330
1335
1340
1345
1350
1355
1360
1365
1370
1375
1380
1385
1390
1395
1400
1405
1410
1415
1420
1425
1430
1435
1440
1445
1450
1455
1460
1465
1470
1475
1480
1485
1490
1495
1500
1505
1510
1515
1520
1525
1530
1535
1540
1545
1550
1555
1560
1565
1570
1575
1580
1585
1590
1595
1600
1605
1610
1615
1620
1625
1630
1635
1640
1645
1650
1655
1660
1665
1670
1675
1680
1685
1690
1695
1700
1705
1710
1715
1720
1725
1730
1735
1740
1745
1750
1755
1760
1765
1770
1775
1780
1785
1790
1795
1800
1805
1810
1815
1820
1825
1830
1835
1840
1845
1850
1855
1860
1865
1870
1875
1880
1885
1890
1895
1900
1905
1910
1915
1920
1925
1930
1935
1940
1945
1950
1955
1960
1965
1970
1975
1980
1985
1990
1995
2000
2005
2010
2015
2020
2025
2030
2035
2040
2045
2050
2055
2060
2065
2070
2075
2080
2085
2090
2095
2100
2105
2110
2115
2120
2125
2130
2135
2140
2145
2150
2155
2160
2165
2170
2175
2180
2185
2190
2195
2200
2205
2210
2215
2220
2225
2230
2235
2240
2245
2250
2255
2260
2265
2270
2275
2280
2285
2290
2295
2300
2305
2310
2315
2320
2325
2330
2335
2340
2345
2350
2355
2360
2365
2370
2375
2380
2385
2390
2395
2400
2405
2410
2415
2420
2425
2430
2435
2440
2445
2450
2455
2460
2465
2470
2475
2480
2485
2490
2495
2500
2505
2510
2515
2520
2525
2530
2535
2540
2545
2550
2555
2560
2565
2570
2575
2580
2585
2590
2595
2600
2605
2610
2615
2620
2625
2630
2635
2640
2645
2650
2655
2660
2665
2670
2675
2680
2685
2690
2695
2700
2705
2710
2715
2720
2725
2730
2735
2740
2745
2750
2755
2760
2765
2770
2775
2780
2785
2790
2795
2800
2805
2810
2815
2820
2825
2830
2835
2840
2845
2850
2855
2860
2865
2870
2875
2880
2885
2890
2895
2900
2905
2910
2915
2920
2925
2930
2935
2940
2945
2950
2955
2960
2965
2970
2975
2980
2985
2990
2995
3000
3005
3010
3015
3020
3025
3030
3035
3040
3045
3050
3055
3060
3065
3070
3075
3080
3085
3090
3095
3100
3105
3110
3115
3120
3125
3130
3135
3140
3145
3150
3155
3160
3165
3170
3175
3180
3185
3190
3195
3200
3205
3210
3215
3220
3225
3230
3235
3240
3245
3250
3255
3260
3265
3270
3275
3280
3285
3290
3295
3300
3305
3310
3315
3320
3325
3330
3335
3340
3345
3350
3355
3360
3365
3370
3375
3380
3385
3390
3395
3400
3405
3410
3415
3420
3425
3430
3435
3440
3445
3450
3455
3460
3465
3470
3475
3480
3485
3490
3495
3500
3505
3510
3515
3520
3525
3530
3535
3540
3545
3550
3555
3560
3565
3570
3575
3580
3585
3590
3595
3600
3605
3610
3615
3620
3625
3630
3635
3640
3645
3650
3655
3660
3665
3670
3675
3680
3685
3690
3695
3700
3705
3710
3715
3720
3725
3730
3735
3740
3745
3750
3755
3760
3765
3770
3775
3780
3785
3790
3795
3800
3805
3810
3815
3820
3825
3830
3835
3840
3845
3850
3855
3860
3865
3870
3875
3880
3885
3890
3895
3900
3905
3910
3915
3920
3925
3930
3935
3940
3945
3950
3955
3960
3965
3970
3975
3980
3985
3990
3995
4000
4005
4010
4015
4020
4025
4030
4035
4040
4045
4050
4055
4060
4065
4070
4075
4080
4085
4090
4095
4100
4105
4110
4115
4120
4125
4130
4135
4140
4145
4150
4155
4160
4165
4170
4175
4180
4185
4190
4195
4200
4205
4210
4215
4220
4225
4230
4235
4240
4245
4250
4255
4260
4265
4270
4275
4280
4285
4290
4295
4300
4305
4310
4315
4320
4325
4330
4335
4340
4345
4350
4355
4360
4365
4370
4375
4380
4385
4390
4395
4400
4405
4410
4415
4420
4425
4430
4435
4440
4445
4450
4455
4460
4465
4470
4475
4480
4485
4490
4495
4500
4505
4510
4515
4520
4525
4530
4535
4540
4545
4550
4555
4560
4565
4570
4575
4580
4585
4590
4595
4600
4605
4610
4615
4620
4625
4630
4635
4640
4645
4650
4655
4660
4665
4670
4675
4680
4685
4690
4695
4700
4705
4710
4715
4720
4725
4730
4735
4740
4745
4750
4755
4760
4765
4770
4775
4780
4785
4790
4795
4800
4805
4810
4815
4820
4825
4830
4835
4840
4845
4850
4855
4860
4865
4870
4875
4880
4885
4890
4895
4900
4905
4910
4915
4920
4925
4930
4935
4940
4945
4950
4955
4960
4965
4970
4975
4980
4985
4990
4995
5000
5005
5010
5015
5020
5025
5030
5035
5040
5045
5050
5055
5060
5065
5070
5075
5080
5085
5090
5095
5100
5105
5110
5115
5120
5125
5130
5135
5140
5145
5150
5155
5160
5165
5170
5175
5180
5185
5190
5195
5200
5205
5210
5215
5220
5225
5230
5235
5240
5245
5250
5255
5260
5265
5270
5275
5280
5285
5290
5295
5300
5305
5310
5315
5320
5325
5330
5335
5340
5345
5350
5355
5360
5365
5370
5375
5380
5385
5390
5395
5400
5405
5410
5415
5420
5425
5430
5435
5440
5445
5450
5455
5460
5465
5470
5475
5480
5485
5490
5495
5500
5505
5510
5515
5520
5525
5530
5535
5540
5545
5550
5555
5560
5565
5570
5575
5580
5585
5590
5595
5600
5605
5610
5615
5620
5625
5630
5635
5640
5645
5650
5655
5660
5665
5670
5675
5680
5685
5690
5695
5700
5705
5710
5715
5720
5725
5730
5735
5740
5745
5750
5755
5760
5765
5770
5775
5780
5785
5790
5795
5800
5805
5810
5815
5820
5825
5830
5835
5840
5845
5850
5855
5860
5865
5870
5875
5880
5885
5890
5895
5900
5905
5910
5915
5920
5925
5930
5935
5940
5945
5950
5955
5960
5965
5970
5975
5980
5985
5990
5995
6000
6005
6010
6015
6020
6025
6030
6035
6040
6045
6050
6055
6060
6065
6070
6075
6080
6085
6090
6095
6100
6105
6110
6115
6120
6125
6130
6135
6140
6145
6150
6155
6160
6165
6170
6175
6180
6185
6190
6195
6200
6205
6210
6215
6220
6225
6230
6235
6240
6245
6250
6255
6260
6265
6270
6275
6280
6285
6290
6295
6300
6305
6310
6315
6320
6325
6330
6335
6340
6345
6350
6355
6360
6365
6370
6375
6380
6385
6390
6395
6400
6405
6410
6415
6420
6425
6430
6435
6440
6445
6450
6455
6460
6465
6470
6475
6480
6485
6490
6495
6500
6505
6510
6515
6520
6525
6530
6535
6540
6545
6550
6555
6560
6565
6570
6575
6580
6585
6590
6595
6600
6605
6610
6615
6620
6625
6630
6635
6640
6645
6650
6655
6660
6665
6670
6675
6680
6685
6690
6695
6700
6705
6710
6715
6720
6725
6730
6735
6740
6745
6750
6755
6760
6765
6770
6775
6780
6785
6790
6795
6800
6805
6810
6815
6820
6825
6830
6835
6840
6845
6850
6855
6860
6865
6870
6875
6880
6885
6890
6895
6900
6905
6910
6915
6920
6925
6930
6935
6940
6945
6950
6955
6960
6965
6970
6975
6980
6985
6990
6995
7000
7005
7010
7015
7020
7025
7030
7035
7040
7045
7050
7055
7060
7065
7070
7075
7080
7085
7090
7095
7100
7105
7110
7115
7120
7125
7130
7135
7140
7145
7150
7155
7160
7165
7170
7175
7180
7185
7190
7195
7200
7205
7210
7215
7220
7225
7230
7235
7240
7245
7250
7255
7260
7265
7270
7275
7280
7285
7290
7295
7300
7305
7310
7315
7320
7325
7330
7335
7340
7345
7350
7355
7360
7365
7370
7375
7380
7385
7390
7395
7400
7405
7410
7415
7420
7425
7430
7435
7440
7445
7450
7455
7460
7465
7470
7475
7480
7485
7490
7495
7500
7505
7510
7515
7520
7525
7530
7535
7540
7545
7550
7555
7560
7565
7570
7575
7580
7585
7590
7595
7600
7605
7610
7615
7620
7625
7630
7635
7640
7645
7650
7655
7660
7665
7670
7675
7680
7685
7690
7695
7700
7705
7710
7715
7720
7725
7730
7735
7740
7745
7750
7755
7760
7765
7770
7775
7780
7785
7790
7795
7800
7805
7810
7815
7820
7825
7830
7835
7840
7845
7850
7855
7860
7865
7870
7875
7880
7885
7890
7895
7900
7905
7910
7915
7920
7925
7930
7935
7940
7945
7950
7955
7960
7965
7970
7975
7980
7985
7990
7995
8000
8005
8010
8015
8020
8025
8030
8035
8040
8045
8050
8055
8060
8065
8070
8075
8080
8085
8090
8095
8100
8105
8110
8115
8120
8125
8130
8135
8140
8145
8150
8155
8160
8165
8170
8175
8180
8185
8190
8195
8200
8205
8210
8215
8220
8225
8230
8235
8240
8245
8250
8255
8260
8265
8270
8275
8280
8285
8290
8295
8300
8305
8310
8315
8320
8325
8330
8335
8340
8345
8350
8355
8360
8365
8370
8375
8380
8385
8390
8395
8400
8405
8410
8415
8420
8425
8430
8435
8440
8445
8450
8455
8460
8465
8470
8475
8480
8485
8490
8495
8500
8505
8510
8515
8520
8525
8530
8535
8540
8545
8550
8555
8560
8565
8570
8575
8580
8585
8590
8595
8600
8605
8610
8615
8620
8625
8630
8635
8640
8645
8650
8655
8660
8665
8670
8675
8680
8685
8690
8695
8700
8705
8710
8715
8720
8725
8730
8735
8740
8745
8750
8755
8760
8765
8770
8775
8780
8785
8790
8795
8800
8805
8810
8815
8820
8825
8830
8835
8840
8845
8850
8855
8860
8865
8870
8875
8880
8885
8890
8895
8900
8905
8910
8915
8920
8925
8930
8935
8940
8945
8950
8955
8960
8965
8970
8975
8980
8985
8990
8995
9000
9005
9010
9015
9020
9025
9030
9035
9040
9045
9050
9055
9060
9065
9070
9075
9080
9085
9090
9095
9100
9105
9110
9115
9120
9125
9130
9135
9140
9145
9150
9155
9160
9165
9170
9175
9180
9185
9190
9195
9200
9205
9210
9215
9220
9225
9230
9235
9240
9245
9250
9255
9260
9265
9270
9275
9280
9285
9290
9295
9300
9305
9310
9315
9320
9325
9330
9335
9340
9345
9350
9355
9360
9365
9370
9375
9380
9385
9390
9395
9400
9405
9410
9415
9420
9425
9430

e. Testing.

ii. Viruses

Control Procedures:

- a. Anti-virus Software;
- b. Currency of Anti-virus Software;
- c. Scanning Practices; and
- d. Scope of Scanning.

2. Financial

Subrisks:

i. Expense Management:

Control Procedures:

- a. Detailed budget;
- b. Expenditure vs. plan; and
- c. Expense Management Report.

3. Information

Subrisks:

i. Restoration

Control Procedures:

- a. Data back-up requirements;
- b. Media worthiness;
- c. Off-site storage;
- d. Back-up performances; and
- e. Back-up testing.

ii. Security

Control Procedures:

- a. Security awareness;
- b. Data guardian;
- c. User ID administration;
- d. Rectification;
- e. User termination procedures;
- f. Violation monitoring;
- g. Dial-up access;
- h. Adherence to standards;
- i. Access approval process;
- j. Testing;
- k. User time-out; and
- l. Data encryption.

4. Legal/Regulatory

Subrisks:

i. Vendor Management

Control Procedures:

- a. Legal counsel;
- b. Escape clauses;
- c. Audit clauses;
- d. Adherence to policies;
- e. Point person established;
- f. Escalation process;
- g. Billing reconciliation; and
- h. Performance reporting.

ii. Software Licensing

Control Procedures:

- a. Awareness;
- b. Software inventory;
- c. Documentation;
- d. Upgrade documentation;
- e. Compliance testing;
- f. Invoices; and
- g. Entitlements - market data access is assigned to users based on contractual agreements.

5. People

Subrisks:

i. Capability

Control Procedures:

- a. Sourcing Strategy;
- b. Staff Retention;
- c. Succession Plans;
- d. Recruiting;
- e. Performance evaluations; and
- f. Attrition.

i. Compliance

Control Procedures:

- a. Diversity;
- b. Core Values;
- c. JPM work authorization;

- d. Adherence to policies; and
- e. Policy Review.

6. Physical Security

Subrisks:

- i. Capability

Control Procedures:

- a. Location Security;
- b. Restricted Access;
- c. Recertification;
- d. Termination process;
- e. Environment controls; and
- f. Power supply.

6. Technology

Subrisks:

- i. Change Management

Control Procedures:

- a. Documented Process;
- b. Process Compliance;
- c. Testing Changes;
- d. Business Communication;
- e. Change Integrity;
- f. Emergency Change Approval;
- g. Planning & Scheduling;
- h. Offsite Change Coordination;
- i. Back out;
- j. Segregation of Duties; and
- k. Business Impact.

- ii. Problem management

Control Procedures:

- a. Documented Process;
- b. Monitoring and Alerts;
- c. Help Desk;
- d. Problem reporting process;
- e. Trend Analysis; and
- f. Problem resolution.

- iii. Strategy

5 Control Procedures:

- a. Business Plans;
- b. Business Sponsorship;
- c. Strategy Alignment;
- d. Strategy Communication;
- e. Project Marketing;
- f. Service Level Agreements;
- g. Project Management; and
- h. Management Reporting.

10 iv. Dependability

15 Control Procedures:

- a. Adherence Standards;
- b. Performance Monitoring;
- c. Service Level Agreements;
- d. Management Reporting;
- e. Capacity Planning;
- f. Hardware Reliability;
- g. Hardware Refresh;
- h. Software Currency;
- i. Level of business impact;
- j. Assets Inventory;
- k. Redundancy; and
- l. Y2K Compliance.

20 25 Figure 4 shows the display of the control procedures 403A - 403E for the

Business Resumption subrisk 402A. The user is provided with a detailed description
404 of each control procedure by selecting one of the descriptive terms 403A - 403E
listed under the associated subrisk.

30 Each control procedure is assigned 205 a weight or control procedure priority
("CP-priority"). In the preferred embodiment, the following CP-priorities are used:
very high=10, high=7, medium=4 and low=1. Each assigned CP-priority is stored in

the rating database 105. Priorities for control procedures are preferably pre-set by an administrator.

The user is prompted to enter (see 405, Figure 4) a compliance rating for each control procedure 206. In the preferred embodiment, these ratings comprise:

5 green=full compliance, yellow=partial compliance, red=non-compliance, and blue=not applicable. For each non-compliance or partial compliance control procedure, the user will be prompted 501 (Figure 5) to determine 208 whether to enter an action plan or accept the risk. For each action plan created 209, the user will enter a description 502, target date 503 and additional comments 504. The user may also enter an estimated cost 505 and assign individuals 506 to the action plan.

In the preferred embodiment, each assessor also associates a number of additional parameters with each subrisk and/or control procedure. For example, the assessor may associate a process, city or region, or organization with each entry.

15 Other parameters would be apparent in other applications. This associated data is stored in the rating database 106 and may be used for sorting and displaying as discussed below.

The compliance score is preferably based on cumulative weighting of two factors: the priority weight of each control procedure ("CP_weight") and the compli-

ance or status factor ("CP_status_factor") for each such control procedure. In the preferred embodiment, this is calculated as:

Subrisk score equals:

$$\sum_{\text{control procedures}} ((\text{CP_weight} / (\sum_{\text{control procedures}} (\text{CP_weight})) * \text{CP_status_factor}) * 10,$$

5 and the overall score equals the average of all the subrisk scores.

where:

$\sum_{\text{control procedures}}$ sums the control procedures for a given subrisk.

CP_weight ranges from:

<u>status</u>	<u>weight</u>
extremely high	scaleable (i.e. 10)
high	scaleable (i.e. 7)
medium	scaleable (i.e. 4)
low	scaleable (i.e. 1)

CP_status_factors range from:

<u>status</u>	<u>weight</u>
full compliance(green)	scaleable (i.e. 10)
partial compliance(yellow)	scaleable (i.e. 4)
non-compliance(red)	scaleable (i.e. 1)
not applicable (blue)	scaleable (i.e. 0)

An example implementation of this scoring system is given in Table I below:

TABLE I

<u>CP_Priority</u>	<u>CPP</u>	<u>Weight</u>

Extr.	(EH)	1.8	
High			
High	(H)	1.1	
Med.	(M)	1	
5	Low	(L)	0.5

<u>Status</u>	<u>Factor</u>
Green	(G) 10
Yellow	(Y) 6
10	Red (R) 2
	Blue (B) 0

scoring

Subrisk	<u>CP</u>	<u>Priority</u>	<u>Weight</u>	<u>Status</u>	<u>Status</u>	<u>Weight %</u>	<u>Status</u>
				<u>Factor</u>			<u>factor x</u>
	A	EH	1.8	G	10	33%	3.33
	B	H	1.1	R	2	20%	0.41
	C	M	1	Y	6	19%	1.11
	D	M	1	G	10	19%	1.85
	E	L	0.5	R	2	9%	0.19
	F	M	0	B	0		
				Total		100%	6.89 Add up
				<u>Weight</u>			scores
				5.4			68.89 Total
							score x
							10

scoring

Subrisk	<u>CP</u>	<u>Priority</u>	<u>Weight</u>	<u>Status</u>	<u>Status</u>	<u>Weight %</u>	<u>Status</u>
				<u>Factor</u>			<u>factor x</u>
	G	EH	1.8	R	2	46%	0.92
	H	H	1.1	R	2	28%	0.56

Patent Apnl. JPM 001

I	L	0.5	G	10	13%	1.28
J	L	0.5	G	10	13%	1.28

Total
Weight
5 3.9 100% 4.05 Add up
scores
40.51 Total
score x
10

scoring

Subrisk C	<u>CP</u>	Priority	<u>Weight</u>	Status	<u>Status</u>	<u>Weight %</u>	<u>Status</u>
					<u>Factor</u>	<u>factor x</u>	<u>weight%</u>
10	K	EH	1.8	R	2	32%	0.63
10	L	EH	1.8	G	10	32%	3.16
10	M	EH	0.5	G	10	9%	0.88
10	N	L	0.5	Y	6	9%	0.53
10	O	M	0	B	0	0%	0.00
10	P	M	0	B	0	0%	0.00
10	Q	H	1.1	G	10	19%	1.93
			Total <u>Weight</u>		100%	7.12 Add up scores	
			5.7			71.23 Total score x	
						10	

20

Overall
Score

Subrisk
A

<u>score</u>	68.89
--------------	-------

Subrisk	40.51
B	
Subrisk	71.23
C	

5

Total	180.63	Divide 180.6/3	60.21
Weight		by # of	
		Sub-	
		risks	
		(e.g. 3)	

Based on the target dates set in the action plans, the system may also optionally calculate 210 future compliance scores. This allows assessors to easily determine whether action plans are aggressive enough or unnecessarily aggressive. This also allows administrators to create a simple metric for determining how well groups perform in meeting their action plans.

The novel system of weighing and categorizing risk of the present invention also facilitates the display of risk data in a number of ways which heretofore had not been possible. For example, compliance scores may be sorted by process (e.g., voice, desktop, midrange, networks, mainframe, market data, etc.) and displayed as shown in Figure 6. As a further example, Figure 7 shows compliance scores for individual subisks sorted by business location. Various other ways of sorting and displaying compliance scores will be apparent to those of skill in the art and include,

for example, compliance scores for individual processes sorted by business organization, or compliance scores for individual business organizations sorted by business location. Such displays are extremely helpful to management in locating weak spots in risk compliance.

5

The system of the present invention also facilitates the ability to predict future levels of compliance and to teach entities ability to meet forecasts. Forecasts versus actual results may be sorted in any of a number of ways. Figure 8 shows the forecast versus actual results for an individual city and individual subrisk. As shown in Figure 9, actual versus target results may be sorted by subrisk and displayed.

0
10
20
30
40
50
60
70
80
90
100

Figure 10 shows an action plan status report for an individual process and individual city. Other reports made possible by the system of the present invention will be understood by those of skill in the art, and include, for example, views showing the number of compliant and non-compliant control procedures sorted by accessing organization.

15

Although the specification and illustrations of the invention contain many particulars, these should not be construed as limiting the scope of the invention but as merely providing an illustration of the preferred embodiments of the invention. For example, while the system is described in terms of risks and subisks, it will be understood by those of ordinary skill in the art based on the specification herein that

the method and system may be utilized using a single category of risks. Moreover, while the described system is described in terms of identifying one or more control procedures for each subrisk element, it will also be understood by those of ordinary skill in the art, based on the specification herein, that the system may be designed to allow assessors to identify non-applicable subisks in which case it would be unnecessary to identify control procedures for such subisks. Thus, the claims should be construed as encompassing all features of patentable novelty that reside in the present invention, including all features that would be treated as equivalents by those skilled in the art.

What is claimed is:

1. A method of managing risk with the aid of a computer system, said method comprising:
 - a. identifying a set of risk elements, said risk elements being stored in a database coupled to said computer;
 - b. identifying one or more control procedures associated with each said risk element, said control procedures being stored in said database;
 - c. assigning a weight to each said control procedure;
 - d. determining a compliance rating for each said control procedure; and
 - e. calculating a compliance score, said compliance score being a function of said assigned weights and said compliance rating of said control procedures.
2. The method of claim 1, wherein said compliance ratings comprise at least one rating identifying a non-fully compliant control procedure, said method further comprising the steps of:
 - a. for each said control procedure having a non-fully compliant rating, receiving a signal indicating whether said non-fully compliant rating is accepted or not accepted; and

5 b. for each said non-fully compliant control procedure which is indicated as not accepted, generating an action plan.

10 3. The method of claim 2 wherein said action plan include a target date, said method further comprising the step of calculating an expected compliance score for one or more future dates based on said action plan target dates.

15 4. The method of claim 3 further comprising the step of tracking whether said expected compliance scores have been met, said tracking including calculating actual compliance scores for said target dates.

5 5. The method of claim 4 further comprising the step of displaying said expected compliance scores versus said actual compliance for said target dates.

10 6. The method of claim 1 further comprising the step of associating one or more parameters with each said compliance rating.

15 7. The method of claim 6 wherein said one or more parameters are selected from the group comprising organization, business line, process, and region.

8. The method of claim 6 further comprising the step of sorting said compliance scores by said one or more parameters.

15 9. The method of claim 8 further comprising the step of displaying said sorted compliance scores.

10. A method of managing risk with the aid of a computer system, said method comprising:

- a. identifying a set of risk elements, said risk elements being stored in a database coupled to said computer;
- 5 b. identifying one or more subrisk elements associated with each said risk element, each said subrisk element being stored in said database;
- c. identifying one or more control procedures associated with each said subrisk element, said control procedures being stored in said database;
- d. assigning a weight to each said control procedure;
- 10 e. determining a compliance rating for each said control procedure, said compliance ratings including a plurality of categories including at least one category indicating said control procedure is not fully compliant;
- f. calculating a compliance score, said compliance score being a function of said assigned weights and said compliance rating of said control procedures;
- 15 g. for each said subrisk, determining whether at least one control procedures associated with said subrisk is not fully compliant;

5

- h. for each said subrisk associated with at least one control procedure which is not fully compliant, receiving a signal indicating whether said subrisk should be accepted or not accepted; and
- i. for each said subrisk which is indicated as not accepted, generating an action plan.

11. The method of claim 10 wherein said action plan further includes a target date, said method further comprising the step of calculating a future compliance score based on said action plan target dates.

12. The method of claim 10 further comprising the step of associating one or more parameters with each said compliance rating.

13. The method of claim 12 further comprising the step of sorting said compliance ratings and displaying said sorted ratings.

14. A method of forecasting risk with the aid of a computer system, said method comprising:

- a. identifying a set of risk elements, said risk elements being stored in a database coupled to said computer;
- b. identifying one or more control procedures associated with each said risk element, said control procedures being stored in said database;
- c. assigning a weight to each said control procedure;

5

- d. determining a compliance rating for each said control procedure, said compliance ratings chosen from a set of ratings including at least one rating identifying a non-fully compliant control procedure and at least one rating identifying fully compliant control procedures;
- e. for each said control procedure having a non-fully compliant rating, generating an action plan, said action plan including a target date for at least one action listed therein; and
- f. calculating an expected compliance score for a future date, said expected compliance score being a function of said assigned weights, said fully compliant control procedures, and said action plan target dates for said non-fully compliant control procedures.

10

15. The method of claim 14 wherein said action plan comprises a signal indicating whether said non-fully compliant rating is accepted or not accepted, said expected compliance score further being a function of said non-fully compliant ratings which have been accepted.

15

16. A data processing system for managing risk, said system comprising:

- a. a database;
- b. a processor coupled to said database, said processor being programmed to perform the steps comprising:

5

- i. receiving a first signal identifying a set of risk elements, said risk elements being stored in said database;
- ii. receive a second signal identifying one or more control procedures associated with each said risk element, said control procedures being stored in said database;
- iii. receive a third signal assigning a weight to each said control procedure, said weight being stored in said database;
- iv. receive a fourth signal identifying a compliance rating for each said control procedure; and
- v. calculate a compliance score, said compliance score being a function of said assigned weights and said compliance rating of said control procedures.

10
15

17. The data processing system of claim 16, wherein said compliance ratings comprise at least one rating identifying a non-fully compliant control procedure, said processor being further programmed to perform the steps comprising:

- a. for each said control procedure having a non-fully compliant rating, receiving a signal indicating whether said non-fully compliant rating is accepted or not accepted;

5

- b. for each said non-fully compliant control procedure which is indicated as not accepted, receiving an action plan, said action plan including an expected target date for implementation and an expected compliance rating; and
- c. generating one or more future expected compliance scores, said compliance scores being a function of said target dates, said assigned weights and said expected compliance rating of said control procedures.

18. The data processing system of claim 16 further comprising a computer display coupled to said processor, said processor further being programmed to display said compliance scores on said computer display.

ABSTRACT

A data processing system and method of using said data processing system for assessing and managing risk is disclosed. The preferred embodiment of the method includes the steps of identifying a set of risk elements; determining an importance for each said risk element; identifying any subisks associated with said risk elements; identifying one ore more control procedures for each said subrisk element; assigning weights to each said control procedure; rating compliance with each said control procedure and calculating an overall weighed compliance score. The method may further include the steps of for each non-fully compliant subrisk, allowing the user to determine whether to accept the risk or generate an action plan addressing the risk. The method may further preferably include calculating future compliance scores based on said action plans. The system further provides for sorting and displaying compliance scores by a number of parameters.

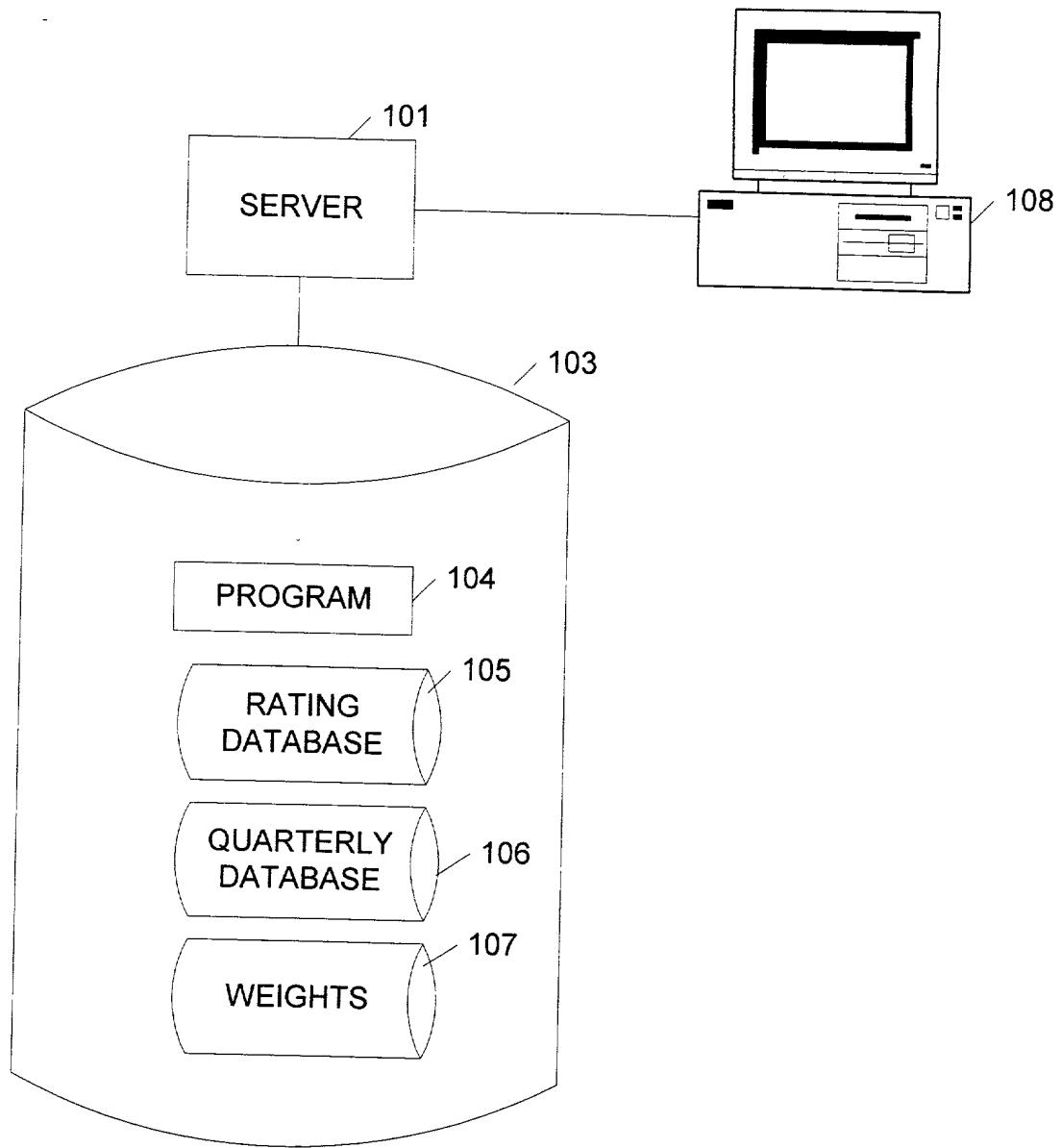
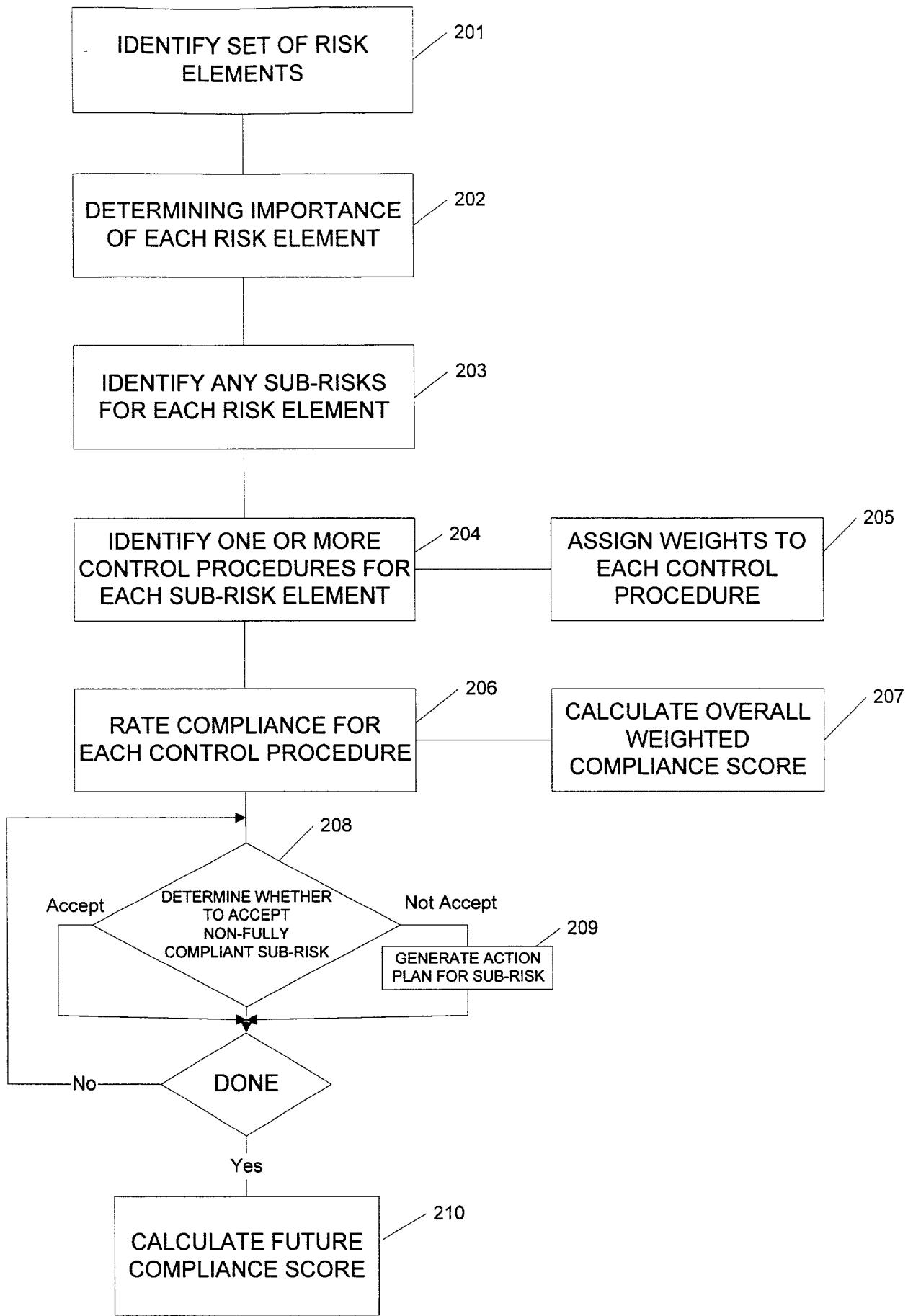


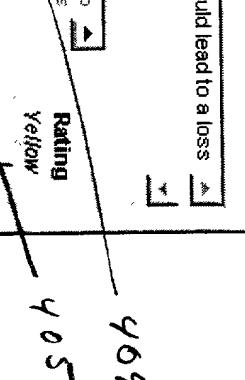
FIGURE 1

Figure 2



Assessments	Scope	Risk Assessment	Risk Detail	Action Plan	Submit																																			
Voice / Tracker Voice / Hong Kong 30/1																																								
<table border="1"> <tr> <td>Risk Rating</td> <td>Business Continuity</td> <td>High</td> <td>Med</td> <td>Low</td> </tr> <tr> <td colspan="5">Financial</td> </tr> <tr> <td colspan="5">Information</td> </tr> <tr> <td colspan="5">Legal/Regulatory</td> </tr> <tr> <td colspan="5">People</td> </tr> <tr> <td colspan="5">Physical Security</td> </tr> <tr> <td colspan="5">Technology</td> </tr> </table>						Risk Rating	Business Continuity	High	Med	Low	Financial					Information					Legal/Regulatory					People					Physical Security					Technology				
Risk Rating	Business Continuity	High	Med	Low																																				
Financial																																								
Information																																								
Legal/Regulatory																																								
People																																								
Physical Security																																								
Technology																																								
Risk Description: The risk that the firm is unable to continue operating in a certain location(s) in the event of a disruption to business.																																								
Policies: <ul style="list-style-type: none"> 1. Business and technology recovery action plans must exist for all businesses, including their associated support functions. Fluid components of the recovery plans (e.g. notification lists) must be updated semi-annually and more static information (e.g. strategies, recovery procedures) must be updated annually. 																																								
<input style="width: 100px;" type="button" value="Save"/>																																								

FIGURE 3

Assessments	Scope	Risk Assessment	Risk Detail	Action Plan	Submit
Business / Trader Voice (Hong Kong)					
Sub-risk description for: Bus. Resum.					
Businesses could be unable to resume if their facilities become unavailable. This could lead to a loss of market share, regulatory penalties and reputational damage.					
Control Procedure 3.5 Off-site Recoverability					
<p>A comprehensive technology recovery plan exists for restoration of this service to another site including duplication of critical items of hardware, software, network and third party services as well as monitoring tools, techniques and documentation.</p>					
					
Gap: (Required)					
<p>A plan exists but is not as comprehensive as listed above</p>					
Additional Comments:					
<p>Partial Compliance</p>					
Scanning Practices					
<p>Scope of Scanning</p>					
<p>1. <input checked="" type="checkbox"/> Financial</p>					
<p>2. <input checked="" type="checkbox"/> Expense Mgt.</p>					
<p>3. <input checked="" type="checkbox"/> Detailed Budget</p>					
<p>Mgmt. Reports:</p>					
<p>R</p>					
<p>Save Reset Create Action Plan View All Action Plans</p>					

FLUORE

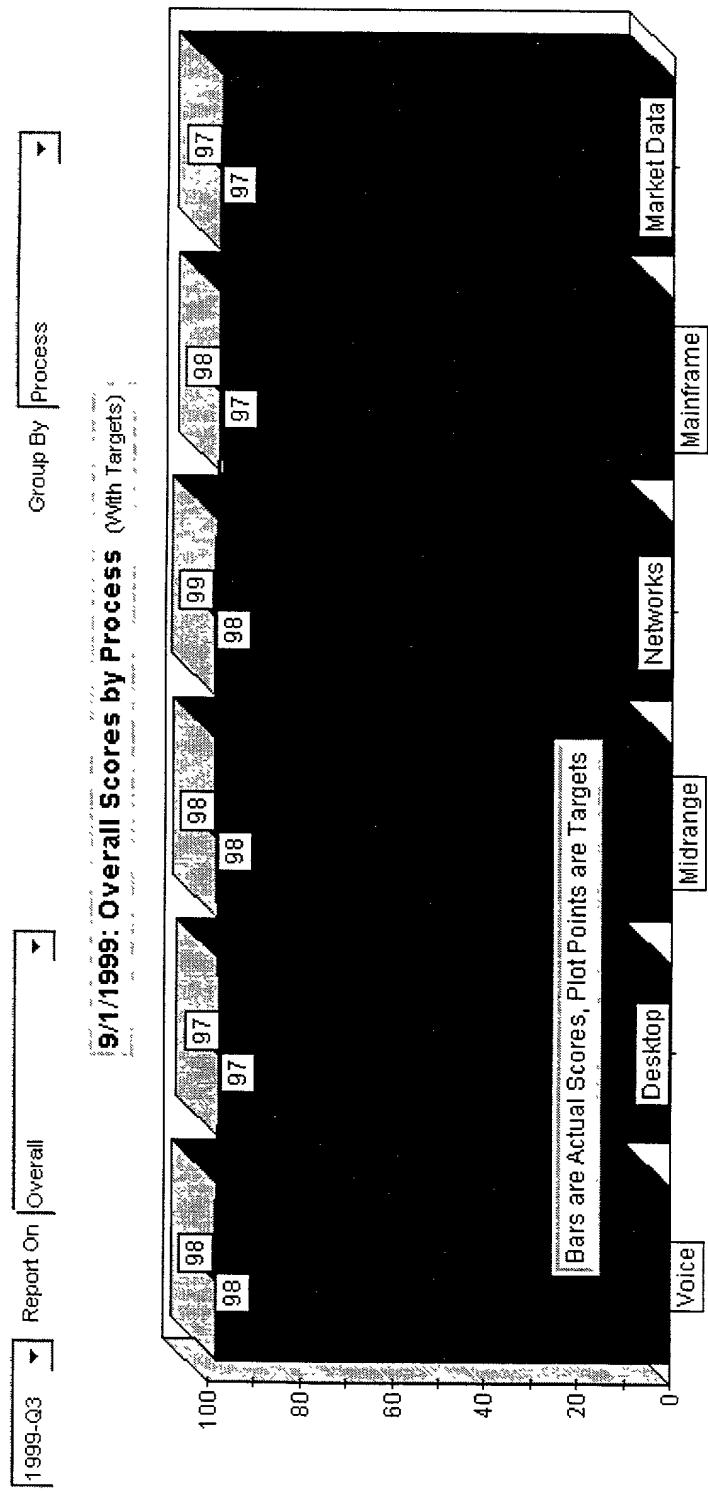
Assessments	Scope	Risk Assessment	Risk Detail	Action Plan	Submit
Voice / Trader Voice / Hong Kong					
Task Name	Subrisk Name	Gap Name	Control Procedure	Action Plan Status	Rating
Business Continuity	Bus. Resum.	A plan exists but is not as comprehensive as required	Off-site Recoverability	Action Plan Created	Yellow
Business Continuity	Bus. Resum.	The last test was conducted	System Testing	Action Plan Created	Yellow
Business Continuity	Bus. Resum.	During the last test we had 51	Test Performance	Action Plan Created	
Business Continuity	Bus. Resum.	During the last test we had 51	Test Performance	Action Plan Created	

Create Action Plan		Accept His	501
Task Search		Status:	Open
Description:	Business Continuity Plan	JOEL	KLEIN
Target Date:	12/15/1999	Est. Cost:	\$5000 - \$505
Action Plan:	We will revise the current plan to include more detail such as - -people		
	<input type="button" value="Save"/> <input type="button" value="New"/> <input type="button" value="Delete"/>		

501
502
503
504
505

504

501
502
503
504
505



51642E1

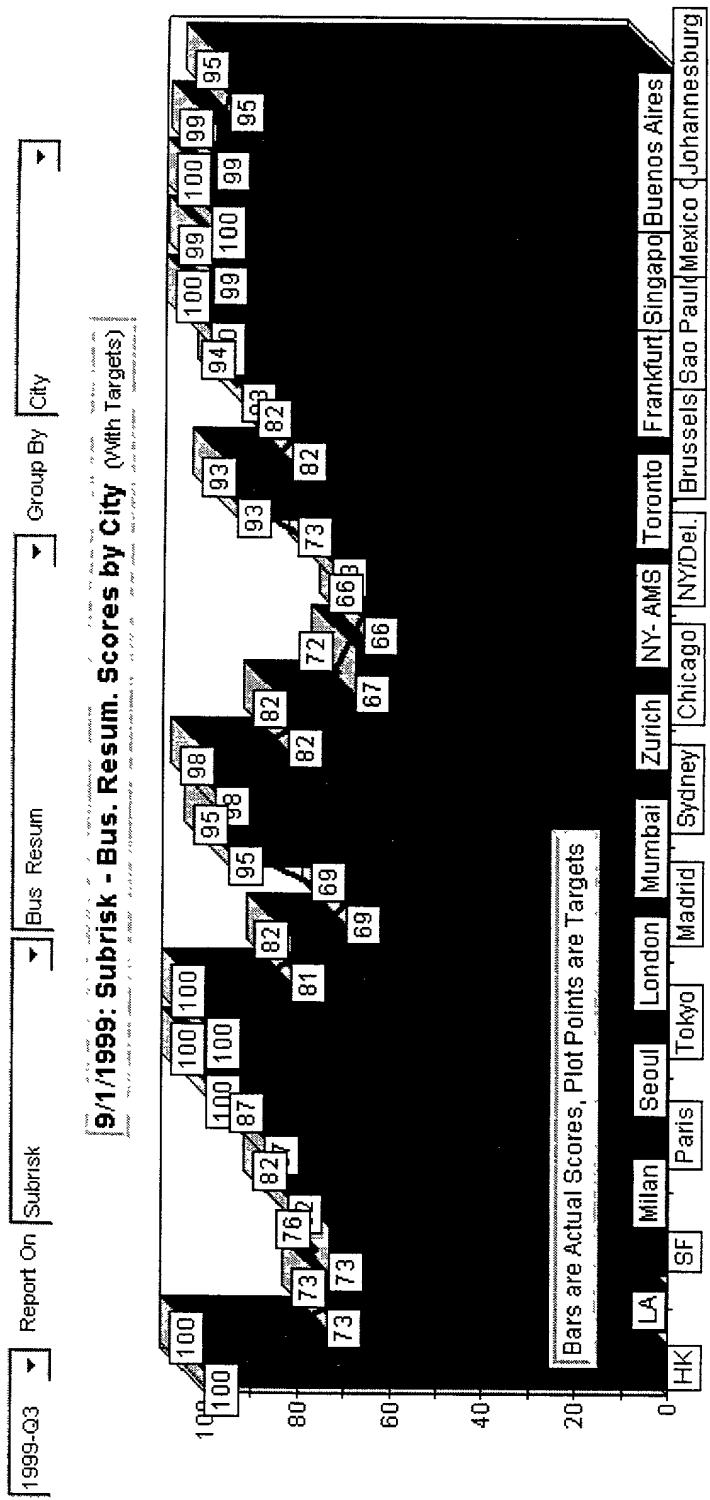
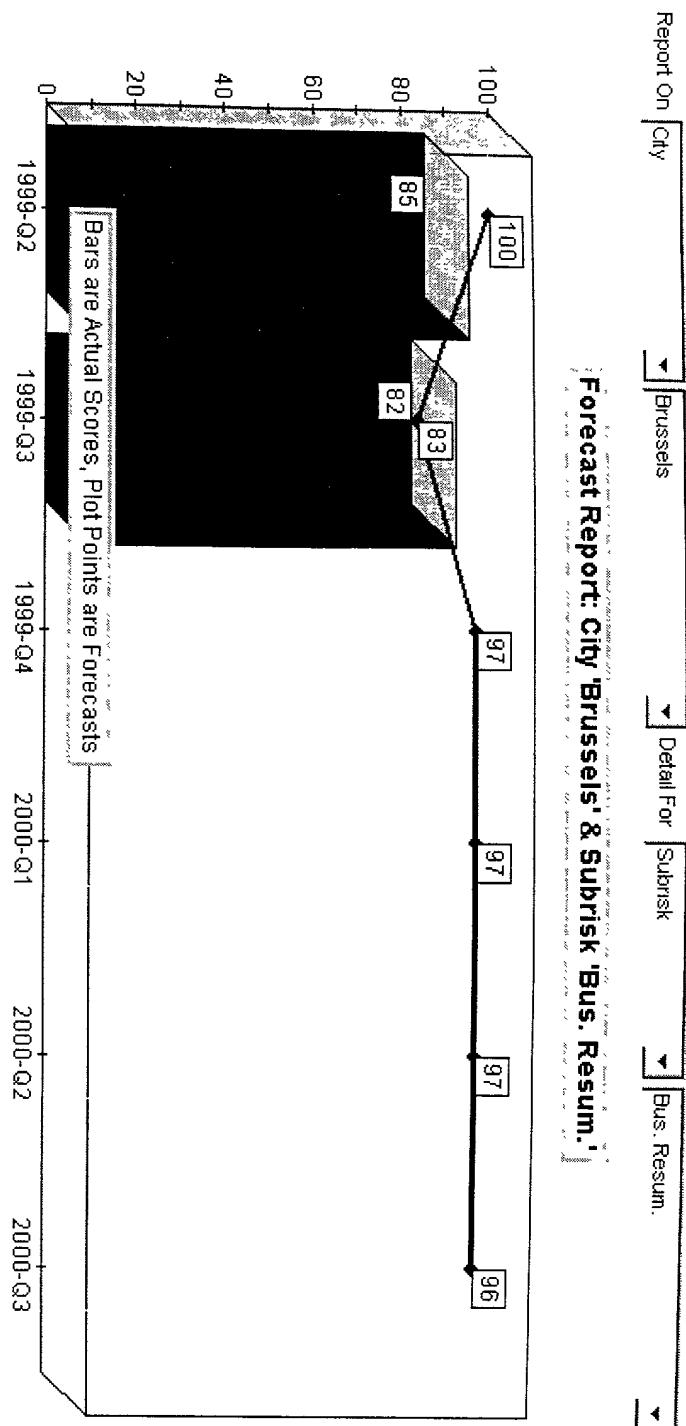


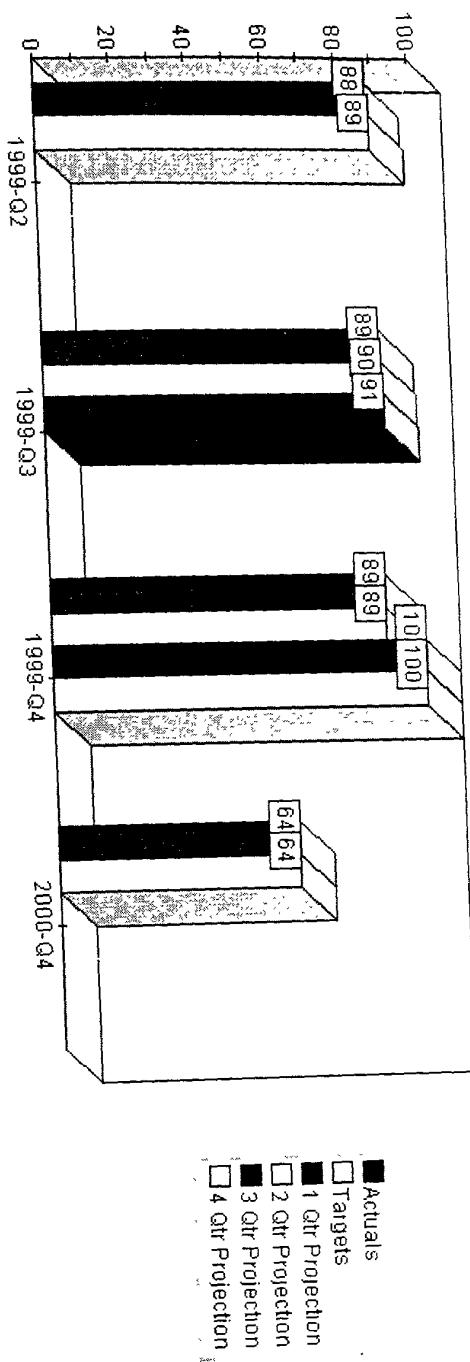
Figure 8

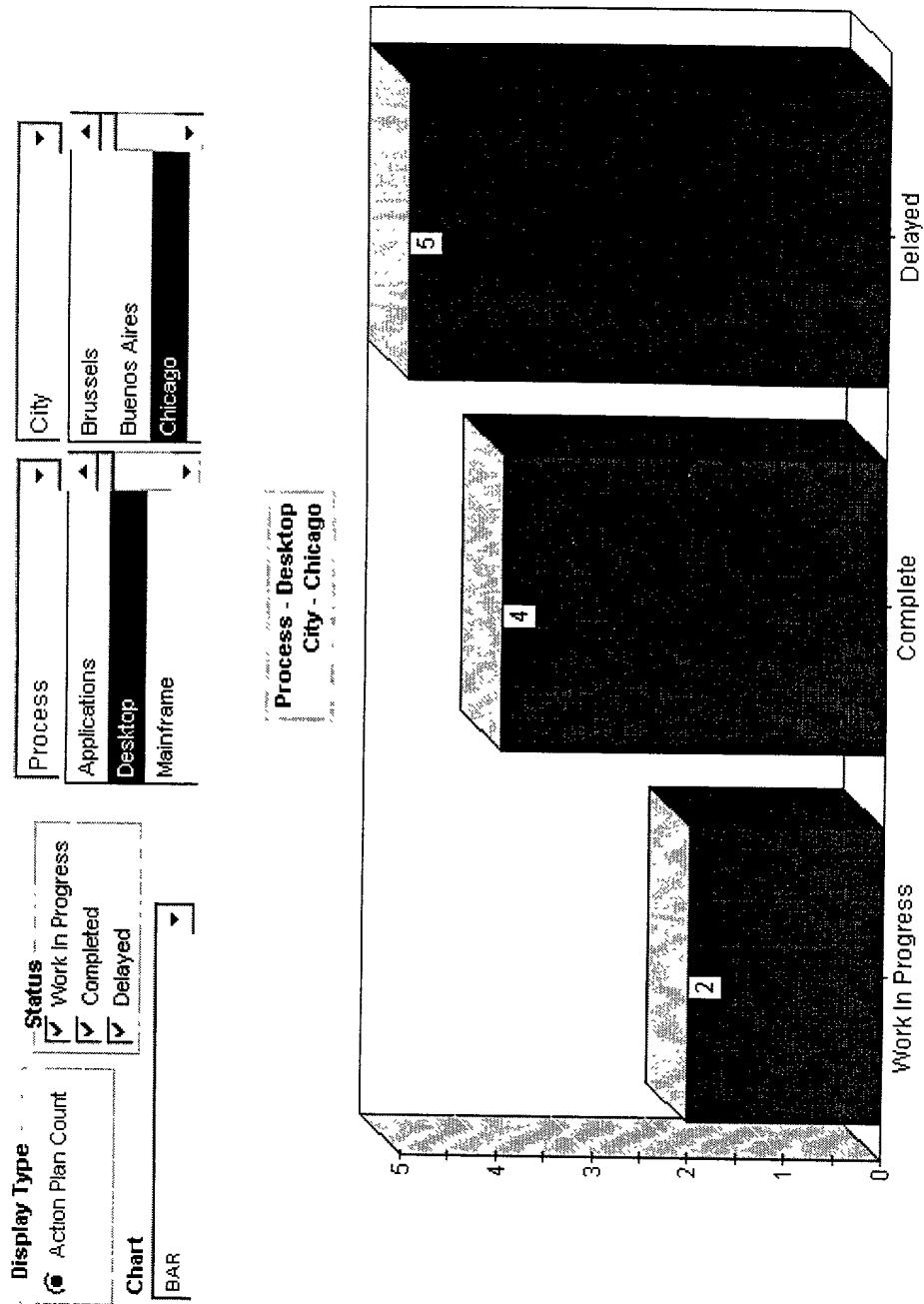


FL-VR-9

Report On Bus Resum Detail For

Actuals vs Targets: Subrisk 'Bus. Resum.' (With Projected Target Scores)





COMBINED DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship is as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled:

Method and System for Managing Risks

the specification of which (check only one item below)

is attached hereto.

was filed as United States Application
on _____

Serial Number _____

and was amended on _____

was filed as PCT international application
on _____

Number _____

and was amended on _____

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with 37 C.F.R. 1.56 (a).

I hereby claim foreign priority benefits under 35 U.S.C. 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(b) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate, or any PCT international application on this invention filed me or my legal representatives or assignees and having a filing date before that of the application on which priority is claimed.

Foreign Application Number(s)	Country	Filing Date	Priority Claimed - (Yes or No)

I hereby claim the benefit under 35 U.S.C. 119(e) of any United States provisional application(s) listed below.

Application Number(s)	Filing Date

POWER OF ATTORNEY

As a named Inventor, I hereby appoint the following attorneys, with full power of substitution and revocation, to prosecute this application and to transact all business in the United States Patent and Trademark Office connected therewith:

Attorney	Registration No.
Daniel A. DeVito	32,125
Edward V. Filardi	25,757
Constance S. Huttner	35,903
Robert B. Smith	28,538
Andrew F. Strobert	35,375
Jose Esteves	41,011
Guy Perry	46,194

Send correspondence and direct telephone calls to:

Andrew F. Strobert
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
Four Times Square
New York, NY 10036,
Telephone No. (212) 735-3000.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further, that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Full Name of First

Joint Inventor: Craig Spielmann

Inventor's signature: Craig R. Spielmann

Date signed: 3/30/00

Inventor Residence and
Post Office Address:

162 Park Street
Montclair, NJ 07042
United States

Citizenship: United States

Full Name of Second

Joint Inventor: Maria Hutter

Inventor's signature: Maria C. Hutter

Date signed: 4/1/00

Inventor Residence and
Post Office Address:

50 Reed Drive South
Princeton Junction, NJ 08550
United States

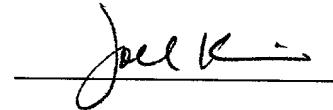
Citizenship: United States

Full Name of Third

Joint Inventor:

Joel Klein

Inventor's signature:



Date signed: 3/31/00

Inventor Residence and
Post Office Address:

27 Ridge Road
Croton, NY 10520
United States

Citizenship:

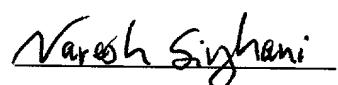
United States

Full Name of Fourth

Joint Inventor:

Naresh Singhani

Inventor's signature:



Date signed: 3/31/00

Inventor Residence and
Post Office Address:

375 Harrison Street
Paramus, NJ 07652
United States

Citizenship:

United States